

**IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI**

**IN THE MATTER OF THE
SEARCH OF
2829 SOUTH LONE PINE AVENUE
SPRINGFIELD, MISSOURI 65804**

18-SW-AUANDPR

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, K. Michael Effland, affiant, being duly sworn under oath, hereby depose and state:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have served in this capacity since May 2017. I am currently assigned to the Kansas City Division, Springfield, Missouri Resident Agency. My duties as a Special Agent include investigating criminal violations of Federal Law.
2. I am a graduate of the FBI's Basic Field Training Course, where I received classroom and practical training. I graduated from The University of Texas with a bachelor's of science degree in Mechanical Engineering in 2009. I have experience in conducting fraud investigations and have received training in the use of computers to commit federal crimes. As part of my duties with the FBI, I investigate criminal violations relating to bank fraud and money laundering, in violation of 18 U.S.C. §§ 1344, 1014, and 1956-57.
3. This affidavit is made in support of a search warrant. The facts contained herein are based upon my own personal knowledge, observations, training and experience,

investigation of this matter, and information and facts related to me by other members of federal and local law enforcement; and what I have learned from other sources specifically detailed herein. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, this affidavit does not contain every fact known to me concerning this investigation.

4. This affidavit has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1344, 1014, and 1956-57 are currently located at 2829 South Lone Pine Avenue, Springfield, Greene County, Missouri 65804, which is located in the Western District of Missouri.
5. This affidavit is made in support of an application for a warrant to search the home of Michael Willhoit, d/b/a Willhoit Enterprises, LLC (hereinafter Willhoit). The property to be searched is further described in the following paragraphs and in Attachment A. Based on the facts set forth herein, I respectfully request the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.
6. As outlined below, and based on my training and experience, I have probable cause to believe that evidence of violations of 18 U.S.C. §§ 1344 (Bank Fraud), 1014 (False Statement on Loan Application), 1956-57 (Money Laundering), and other criminal statutes is located in and within the property described in paragraph 4.

II. CRIMINAL STATUTES VIOLATED

7. Under 18 U.S.C. § 1344: “Whoever knowingly executes, or attempts to execute, a scheme or artifice (1) to defraud a financial institution or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises; shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both.”
8. Under 18 U.S.C. § 1956: “Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity with the intent to promote the carrying on of specified unlawful activity; or with the intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, of the control of the proceeds of specified unlawful activity; or to avoid a transaction reporting requirement under State or Federal law; shall be fined not more than \$500,000 or twice the value of the property involved in the transaction whichever is greater, or imprisoned not more than twenty years, or both.”
9. Under 18 U.S.C. § 1957: “Whoever, knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000

and is derived from specified unlawful activity, shall be fined, or imprisoned not more than ten years, or both.”

10. Under 18 U.S.C. § 1014: “Whoever knowingly makes any false statement or report, or willfully overvalues any land, property, or security, for the purpose of influencing in any way the action of...any institution the accounts of which are insured by the Federal Deposit Insurance Corporation,...upon any application, advance, discount, purchase, purchase agreement, repurchase agreement, commitment, loan, or insurance agreement or application for insurance or a guarantee, or any change or extension of any of the same, by renewal, deferment or action or otherwise, or the acceptance, release, or substitution of security therefore, shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both.”

III. BACKGROUND ON COMPUTERS

11. Based on my knowledge, training, experience, and information relayed to me by agents and others involved in the forensic examination of computers, I know the following:
 - a. Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical or similar computer impulses or data. Hardware includes any data-processing devices (such as central processing units and self-contained “laptop” or “notebook” computers); internal and peripheral storage devices (such as fixed disks, floppy disks, external hard disks, floppy disk drives and

diskettes, tape drives and optical storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts, that can be used to restrict access to computer hardware (such as physical lock and keys).

- b. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs.
- c. Computer-related documentation consists of written, recorded, printed, or electronically-stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.
- d. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or programming codes. A password (which is a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security

hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- e. Computer hardware and computer software may be utilized to store information or data in the form of electronic or magnetic coding on computer media or on media capable of being read by a computer or computer related equipment. This media includes, but is not limited to fixed hard drives and removable hard drive cartridges, laser disks, tapes, floppy disks, CD-ROMs, and any other media capable of storing magnetic coding.
- f. In this case, because several people have shared the premises as a residence, it is possible that the premises will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

12. Based on my knowledge, training, experience, and information relayed to me by agents and others involved in forensic examination of computers, I know that searching and seizing information from computers often requires agents to seize most or all electronic-storage devices, along with related peripherals, to be searched later by a qualified expert in a laboratory or other controlled environment for the following reasons:

- a. The volume of evidence. Computer storage devices (like hard disks, diskettes, thumb drives, tapes, and laser disks) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.
- b. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive

code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

- c. Searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer’s input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the computer’s data in a laboratory or other controlled environment. This is true because of the following;
- d. The peripheral devices which allow the users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many systems storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the computer as it now operates in order to accurately retrieve the evidence.
- e. In addition, the analyst needs the relevant system software (operating systems, interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals, or other documentation and data security devices.

IV. DEFINITIONS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. The term “computer”, as defined in 18 U.S.C § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.
- b. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, iPods, iPhones, iPads, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to,

physical key and locks).

- c. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- d. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.
- e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hides, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

- f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- g. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

V. COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. As described above, this application seeks permission to search for records that might be found on each location at the specified target location as identified above

in whatever form they are found. One possible form that the records could be contained and found, is as data stored on a computer's hard drive or as other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

15. I submit that if a computer or storage medium is found, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, the files can be recovered months or years later using forensic tools. This is because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, the data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a

record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media, in particular, a computer’s internal hard drives contain electronic evidence of how a computer has been used, what it has been used for, and who has used the device. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is required for such a task. However, it is technically possible to delete this information.
 - d. Similarly, files that have been viewed via the Internet are sometimes downloaded into a temporary Internet directory or “cache.”
 - e. Based on actual inspection of other evidence related to this investigation, financial records, and invoices, I am aware that computer equipment can be used to generate, store, and print documents used in the criminal enterprise scheme. There is reason to believe that there is a computer system currently located at the target location.
16. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that established how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic

electronic evidence will be on any storage medium at the target location because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing,

such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. In most cases, a thorough search of the target locations for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded to the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:
18. The time required for a thorough and complete examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
19. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them may require tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze any system, storage device, and the data discovered during the search. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

20. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

VI. FACTS SUPPORTING PROBABLE CAUSE - FRAUD INVESTIGATION

22. The investigation involving Michael Willhoit, doing business as Willhoit Enterprises, LLC, hereinafter “Willhoit”, began on March 14, 2018, upon the receipt

of a complaint from Wood & Huston Bank. Wood & Huston provided information that Willhoit had obtained loans to purchase vehicles in the normal course of operating his high-end, luxury, used-car business. Willhoit subsequently sold those vehicles out of trust, i.e. without using the proceeds of the sales to pay back the loans, and owes the bank approximately \$1,300,000.

23. According to his website, Willhoit operates a high-end, luxury, used car business specializing in the sale of classic Porsches and other exotic cars. Until April of 2018, Willhoit conducted business from a storefront shared with Premier Sports Cars located at 1950 Chestnut Expressway in Springfield, Missouri.
24. To operate the business, Willhoit obtained loans from several banks to purchase vehicles for resale. These loans were based on documentation, including car titles and purchase agreements, which Willhoit provided to show the purchase of specific vehicles. When the vehicles were sold through the course of his business, Willhoit agreed to and represented to each financial institution that he would immediately repay each loan upon the sale of the vehicle.
25. On March 28, 2018, officials at the Bank of Missouri advised investigators that Willhoit had ten outstanding loans with the Bank of Missouri for the purpose of purchasing cars. The total of the ten outstanding loans is approximately \$1,300,000. Officials advised that in February of 2018, Willhoit informed them that all cars in his possession had been sold and he would be re-paying his financial obligations soon. Willhoit later told the bank that he needed to sell his house in order to pay off

his debts. Thus far, the Bank of Missouri has not been repaid.

26. On April 13, 2018, officials at Old Missouri Bank advised investigators that Willhoit had four outstanding loans with Old Missouri Bank for the purpose of purchasing cars. The total of the four outstanding loans is approximately \$536,510. In March of 2018, Old Missouri Bank officials contacted Willhoit in an effort to schedule an inventory inspection, something that is routinely done in the used-car business. These inspections are conducted to allow the bank to verify the condition and locations of collateral (vehicles purchased with loan proceeds). Willhoit told Old Missouri Bank officials that it was not necessary to conduct an inspection as he had sold all vehicles out of trust and the vehicles were no longer in his possession. Thus far, Old Missouri Bank has not been repaid.

27. On April 27, 2018, officials with Freedom Bank of Southern Missouri advised investigators that Willhoit had ten outstanding loans with Freedom Bank for the purpose of purchasing cars. The total of the ten outstanding loans is approximately \$913,730. On March 13, 2018, officials with Freedom Bank met with Willhoit at his place of business located at 1950 Chestnut in Springfield, Missouri. The officials noted that the cars they normally saw displayed in the showroom were absent. Willhoit told Freedom Bank that he sold the cars out of trust and used the funds to pay for personal expenses, including maintenance on his home and debts to the Internal Revenue Service. Additionally, Willhoit told Freedom Bank officials that several of the titles he had submitted to obtain loans were fraudulent and that he

never purchased the designated vehicles. Thus far, Freedom Bank has not been repaid.

28. On May 22, 2018, officials with Ozark Bank advised investigators that Willhoit had two outstanding loans with Ozark Bank for the purpose of purchasing cars. The total of the two outstanding loans is approximately \$195,000. In March of 2018, Ozark Bank attempted to schedule an inventory inspection with Willhoit without success. On May 21, 2018, Willhoit sent Ozark Bank officials an email stating he had no money to repay his debt, confirming that the two vehicles had been sold out of trust. Thus far, Ozark Bank has not been repaid.
29. The cumulative loss amount to these five banks is approximately \$4,248,000.
30. Grand jury subpoenas were sent to numerous financial institutions, including the victim banks. Investigators obtained relevant records possessed in the normal course of business including loan documents and financial activity related to Willhoit. A review of these documents showed Willhoit owed money relating to the reported purchase of approximately 33 different cars.
31. As an example, Willhoit obtained a \$171,500 loan from Freedom Bank to purchase a 2014 Porsche GT3, VIN: WP0AC2A9XES183200. This loan was obtained on September 20, 2017, and paid back on October 13, 2017. As part of the loan application process, Willhoit provided Freedom Bank with a copy of a California title dated February 11, 2014 and a purchase agreement between Willhoit and a seller "D.D." in California dated September 18, 2017. On November 17, 2017,

Willhoit obtained a \$160,020 loan for the same car, a 2014 Porsche GT3, VIN: WP0AC2A9XES183200 from Wood & Huston Bank. Wood & Huston has not received any repayment. Through internet research, it was found that this particular car, VIN: WP0AC2A9XES183200 is currently for sale at a dealership in Atlanta, Georgia. A salesman at the dealership was interviewed and stated the dealership had taken possession of the car in May of 2018 from a long-term client who had owned the GT3 continuously since December of 2016. Further, the owner had purchased the car from a dealer in Ohio. Open source records checks on the title of this car show that it was titled in Springfield, Missouri, in March of 2014 before being re-titled in Ohio and then Georgia. In summary, although Willhoit, through the course of his business, did have possession of this particular Porsche GT3 in 2014, he submitted false documentation, including an outdated copy of the vehicle title and a false purchase agreement, to Wood & Huston Bank and Freedom Bank in 2017 to obtain a loan that was never used to purchase the vehicle.

VII. EXISTENCE OF RECORDS AT THE TARGET LOCATION

32. Federal agents contacted Willhoit on July 30, 2018, at the property located at 2829 South Lone Pine Avenue, Springfield, Missouri. While there, Willhoit confirmed he was currently living at the residence. Further, multiple news articles report Willhoit renovating, living at, and promoting the home. Willhoit's website currently lists the home for sale.
33. Officials with Ozark Bank advised investigators that Willhoit was no longer


conducting business from the showroom located at 1950 Chestnut Expressway in Springfield, Missouri. In fact, the Willhoit Enterprises sign had been removed from the window. Through personal observation, investigators confirmed that Willhoit no longer conducted business from this location.

34. Willhoit's wife, Lisa Willhoit, was interviewed by investigators on August 7, 2018. She stated that Willhoit was broke, had no cars in his possession, and had effectively shut down Willhoit Enterprises. After Willhoit moved out of the 1950 Chestnut Expressway location, where he could no longer afford to pay rent, he stored all materials, including files, records, and computer equipment, associated with the business in the spare bedroom of their home located at 2829 South Lone Pine Avenue in Springfield, Missouri. Lisa Willhoit stated that Michael Willhoit had spent a considerable amount of time during the last several weeks going through records and files, and throwing some materials away.

VIII. CONCLUSION

35. Based on the foregoing facts contained within this affidavit, and on my experience and training, there is probable cause to believe that at the premises described herein, there is presently concealed those items set forth in Attachment B, which constitute evidence of violations of 18 U.S.C. §§ 1344 (Bank Fraud), 1014 (False Statement on Loan Application), 1956-57 (Money Laundering), and other sections of the United States criminal statutes. Wherefore, I request a search warrant be issued for, and authority be given to seize from the aforementioned location described in

Attachment A (including any attachments, outbuilding, appurtenances thereto, vehicles found on the premises), and any occupants found therein, property constituting evidence of the commission of criminal offenses and fruits, instrumentalities and other evidence and property designed to commit such offenses.



K. Michael Effland
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me this 4th day of September, 2018.



HONORABLE DAVID P. RUSH
United States Magistrate Judge
Western District of Missouri